06-19-00

A

PTO/SB/05 (2/98) (modified)
Approved for use through 9/30/2000, OMB 0651-0032
Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE

NEW UTILITY PATENT APPLICATION TRANSMITTAL

(only for new nonprovisional applications under 37 CFR 1.53(b))

Attorney Docket Number	5015
First Named Inventor	Daniel Schreiber
Total Pages in this Submission	37
Express Mail Label No.	EL482473473US

APPLICATION ELEMENTS

1. ☒ Fee Transmittal Form (in duplicate)
   ☒ Check Enclosed
2. ☒ Specification
   (preferred arrangement set forth below)
   - Descriptive Title of the Invention
   - Cross Reference(s) to Related Case(s)
   - Statement Regarding Fed sponsored R & D
   - Background of the Invention
   - Brief Summary of the Invention
   - Brief Description of the Drawing(s)
   - Detailed Description
   - Claim or Claims
   - Abstract of the Disclosure
3. ☒ Drawing(s) *(when necessary per 35 USC 113)*
4. Oath or Declaration
   a. ☐ New Declaration
      ☐ Executed
   b. ☒ Copy from a prior application (37 CFR 1.63(d))
      (for continuation/divisional with Box 17 completed)
      i. ☐ DELETION OF INVENTOR(S)
      Signed statement attached deleting inventor(s) named in the prior application, see 37 CFR 1.63(d)(2) and 1.33(b).
5. ☒ Incorporation by Reference *(useable if Box 4b is checked)*. The entire disclosure of the prior application, from which a copy of the oath or declaration is supplied under Box 4b, is considered as being part of the disclosure of the accompanying application and is hereby incorporated by reference therein.

ACCOMPANYING APPLICATION PARTS

6. ☐ Assignment & Assignment Recordation Cover Sheet
7. ☐ Certified Copy of Priority Document(s)
   (if foreign priority is claimed)
8. ☐ Information Disclosure Statement & PTO-1449
   ☐ Copies of IDS Citation(s)
9. ☒ Preliminary Amendment
10. Small Entity Statement
    ☐ New Statement enclosed
    ☒ Statement filed in prior application. Status still proper and desired
11. ☒ Return Postcard
12. ☐ _____
13. ☐ _____
14. ☐ _____
15. ☐ _____
16. ☐ _____

ADDRESS TO:

Box Patent Application
Commissioner for Patents
Washington, D.C. 20231

17. **If a CONTINUING APPLICATION,** *check appropriate box and supply the requisite information below and in a preliminary amendment:*
☐ Continuation ☒ Divisional ☐ Continuation-in-part (CIP) of prior application No: 09/313,067
Prior application information: *Examiner:* B. Bonzo *Group/Art Unit:* 2785

18. CORRESPONDENCE ADDRESS

NAME	Laura A. Majerus Fenwick & West LLP				
ADDRESS	Two Palo Alto Square				
CITY	Palo Alto	*STATE*	CA	*ZIP CODE*	94306
COUNTRY	U.S.A.	*TELEPHONE*	(650) 858-7152	*FAX*	(650) 494-1417

Name (Print/Type)	Laura A. Majerus	*Registration No. (Attorney/Agent)*	NO. 33,417
Signature	Laura Majerus	*Date*	6/16/00

Applicant or Patentee: _____ Attorneys Docket No.: 6866-101XX
Serial or Patent No.: _____
Filed or Issued: _____
For: _____

VERIFIED STATEMENT [DECLARATION] CLAIMING SMALL ENTITY STATUS (37 CFR 1.9(f) and 1.27(c)) - SMALL BUSINESS CONCERN

I hereby declare that I am

[ ] the owner of the small business concern identified below;
[X] an official of the small business concern empowered to act on behalf of the concern identified below:

NAME OF CONCERN CSafe Ltd.
ADDRESS OF CONCERN P.O. Box 2361, Beit Shemesh 99543, Israel

I hereby declare that the above identified small business concern qualifies as a small business concern as defined in 13 CFR 121.3-18, and reproduced in 37 CFR 1.9(d), for purposes of paying reduced fees under section 41(a) and (b) of Title 35, United States Code, in that the number of employees of the concern, including those of its affiliates, does not exceed 500 persons. For purposes of this statement, (1) the number of employees of the business concern is the average over the previous fiscal year of the concern of the persons employed on a full-time, part-time or temporary basis during each of the pay periods of the fiscal year, and (2) concerns are affiliates of each other when either, directly or indirectly, one concern controls or has the power to control the other, or a third party or parties controls or has the power to control both.
I hereby declare that rights under contract or law have been conveyed to and remain with the small business concern identified above with regard to the invention entitled METHODS & APPARATUS FOR PREVENTING REUSE OF TEXT, IMAGES AND SOFTWARE TRANSMITTED VIA NETWORKS, by inventor(s) Daniel Schreiber and David Guedaliah
described in

[X] the specification filed herewith
[ ] application serial no._____, filed _____
[ ] patent no. _____, issued _____

If the rights held by the above identified small business concern are not exclusive, each individual, concern or organization having rights to the invention is listed below and no rights to the invention are held by any person, other than the inventor, who could not qualify as a small business concern under 37 CFR 1.9(d) or by any concern which would not qualify as a small business concern under 37 CFR 1.9(d) or a nonprofit organization under 37 CFR 1.9(c). *NOTE: Separate verified statements are required from each named person, concern or organization having rights to the invention averting to their status as small entities. (37CFR 1.27).

FULL NAME _____
ADDRESS _____
[ ] INDIVIDUAL [ ] SMALL BUSINESS CONCERN [ ] NONPROFIT ORGANIZATION

FULL NAME _____
ADDRESS _____
[ ] INDIVIDUAL [ ] SMALL BUSINESS CONCERN [ ] NONPROFIT ORGANIZATION

I acknowledge the duty to file, in this application or patent, notification of any change in status resulting in loss of entitlement to small entity status prior to paying, or at the time of paying, the earliest of the issue fee or any maintenance fee due after the date on which status as a small entity is no longer appropriate. (37 CFR {1.28(b)).
I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under section 1001 of Title 18 of the United States Code, and that such willful false statements may jeopardize the validity of the application, any patent issuing thereon, or any patent to which this verified statement is directed.

NAME OF PERSON SIGNING Daniel Schreiber
TITLE OF PERSON OTHER THAN OWNER Managing Director
ADDRESS OF PERSON SIGNING 71, 71 Shamon St Beit Shemesh

SIGNATURE _____ DATE 9/5/99

IN THE UNITED STATES

PATENT AND TRADEMARK OFFICE

APPLICANTS:	Daniel Schreiber and David Guedaliah
SERIAL NO.:	not yet known
FILING DATE:	June 16, 2000
TITLE:	Method and Apparatus for Preventing Reuse of Text, Images and Software Transmitted Via Networks
EXAMINER:	not yet known
GROUP ART UNIT:	not yet known
ATTY. DKT. NO.:	5015

BOX: PATENT APPLICATION
ASSISTANT COMMISSIONER FOR PATENTS
WASHINGTON, DC. 20231

PRELIMINARY AMENDMENT

SIR:

Prior to the examination of the divisional patent application identified above, please amend this application as follows:

In the Specification before line 1, add--This application is a divisional application of U.S. Application Serial No. 09/313,067 of Schreiber et al., filed May 17, 1999.--

In the Claims:

Please cancel claims 1-11 and 19-26. For the Examiner's convenience, the remaining claims are set forth below:

12. A method for limiting the operational life of software in a network environment, the method comprising:

providing a software application with an associated password to a client via a network;

receiving a request for information from said software application via said network, said request comprising said associated password;

authenticating said password;

providing said information to said software application via said network while said associated password is valid; and

invalidating said password coincident with an invalidation event.

13. A method according to claim 12 wherein said invalidating step comprises invalidating said password at a predetermined time.

14. A method according to claim 12 wherein said invalidating step comprises invalidating said password after a predetermined elapsed time from when said request was received.

15. A method according to claim 12 wherein said invalidating step comprises invalidating said password upon the detection of a loss of communication with said client.

16. A method according to claim 12 wherein said providing step comprises providing said software application in the form of an applet.

17. A method according to claim 12 wherein said providing step comprises providing said password assembled with said software application.

18. A method according to claim 12 wherein said providing step comprises generating said password at a server upon receiving said request at said server.

27. A network-based software authentication system comprising:

a server comprising:

a password generator;

password validation apparatus;

a restricted-access storage area;

a software application; and

invalidation apparatus;

wherein said server is operative to:

a) cause said password generator to generate a password;

b) provide said software application with said password to a client via a network;

c) received a request for information from said software application via said network, said request comprising said associated password;

d) authenticate said password using said password validation apparatus;

e) provide said information to said software application via said network while said associated password is valid; and

f) invalidate said password using said invalidation apparatus coincident with an invalidation event.

28. A system according to claim 27 wherein said invalidation event comprises the arrival of a predetermined time.

29. A system according to claim 27 wherein said invalidation event comprises the elapsing of a predetermined elapsed time from when said request was received.

30. A system according to claim 27 wherein said invalidation event comprises the detection of a loss of communication with said client.

31. A system according to claim 31 wherein said software application comprises an applet.

32. A system according to claim 27 wherein said password is assembled with said software application.

33. A system according to claim 27 wherein said password is generated at said server upon receiving said request at said server.

REMARKS

This application contains the claims of Group III of the parent application.

Favorable action is solicited.

Respectfully submitted,
Daniel Schreiber and David Guedaliah

Dated: 6/16/00

By: Laura Majerus

Laura A. Majerus, Reg. No.: 33,417
Fenwick & West LLP
Two Palo Alto Square
Palo Alto, CA 94306
Tel.: (650) 858-7152
Fax.: (650) 494-1417

21939/04691/DOCS/1057873.1

FIELD OF THE INVENTION

The present invention relates to network security in general and particularly to methods and apparatus for preventing unauthorized reuse of text, images, and software transmitted via networks.

BACKGROUND OF THE INVENTION

Sending text, images, and software via communications networks, particularly computer networks, is known. In one well known network protocol, the Hypertext Transport Protocol or HTTP, best known as a transport protocol for the Internet-based World Wide Web or WWW, a computer terminal or "client" connected to a network, such as the Internet, typically sends a request using software known as a "browser" to a server also connected to the network. Such requests may be for "Web pages," documents constructed using Hypertext Markup Language or HTML and stored at the server, which are then rendered by the client browser into text and/or images. Other requests may be for software applications such as "applets" which are executed by an application engine at the client. Upon receiving a request, the server sends that which was requested to the client.

Preventing unauthorized reuse of text, images, and software provided via networks is difficult given the current state of the art. Text is usually provided in text-editable format which may be copied and reused at the client. While text may be converted to a graphic image at the server and thus provided in a non-text-editable format to the client, this is not practicable both due to the increased storage required to store text as graphic images on the server, as well as the dynamic nature of requests such as search queries where the text results are not known until the query is executed and, therefore, the text cannot be converted to a graphic ahead of time. Images may be captured at the client from the client's video buffer and reused. Software applications including

applets may be decompiled and reused at a later date where a time-limited or access-limited use was originally intended.

SUMMARY OF THE INVENTION

The present invention seeks to provide improved methods and apparatus for preventing unauthorized reuse of text, images, and software transmitted via networks. Text documents, and particularly HTML documents, from which text can be copied are rendered into non-text-editable graphical images at the server upon receiving a request from a client. Graphic images are rendered into a number of sub-images at the server upon receiving a request from a client. The sub-images are then sent to the requesting client together with an applet for displaying the sub-images in a manner that is visually perceived to substantially resemble the graphical image but which cannot be copied simply by taking a snapshot of the client's video buffer. Software applications including applets are provided with an embedded password that may be authenticated by a server to allow access to information for a limited time or under limited conditions. The password is invalidated at a predetermined time of based upon certain conditions, thus preventing future reuse and access to server information.

There is thus provided in accordance with a preferred embodiment of the present invention a method for providing textual information in a network environment, the method including receiving a request via a network for text-editable textual information, converting the text-editable textual information into a non-text-editable textual format on line upon receiving the request, and sending the non-text-editable textual information via the network.

Further in accordance with a preferred embodiment of the present invention the converting step includes converting the text-editable textual information into a non-text-editable graphical representation of the text-editable textual information.

Still further in accordance with a preferred embodiment of the present invention the converting step includes converting the text-editable textual information into the non-text-editable graphical representation the graphical representation includes at least one hyperlink.

Additionally in accordance with a preferred embodiment of the present invention the method further includes displaying the non-text-editable textual information via a computer terminal display.

Moreover in accordance with a preferred embodiment of the present invention the receiving step includes receiving the request from a computer terminal connected to the network at a server connected to the network, the converting step is performed at the server, and the sending step includes the server sending the non-text-editable textual information to the computer terminal via the network.

There is also provided in accordance with a preferred embodiment of the present invention a method for providing graphical information in a network environment, the method including receiving a request via a network for a graphical image, rendering the graphical image into a plurality of sub-images on line upon receiving the request, the sub-images are displayable in a manner that is visually perceived to substantially resemble the graphical image, and displaying the plurality of sub-images in the manner on a display via a video buffer the video buffer includes no more than one of the sub-images in its entirety at any given time.

Further in accordance with a preferred embodiment of the present invention the rendering step includes rendering the graphical image into a plurality of color separations of the graphical image.

Still further in accordance with a preferred embodiment of the present invention the rendering step includes rendering the graphical image into a plurality of sub-images the any of the plurality of sub-images includes an interference pattern.

Additionally in accordance with a preferred embodiment of the present invention the method further includes sending the plurality of sub-images via the network.

Moreover in accordance with a preferred embodiment of the present invention the displaying step includes displaying the plurality of sub-images via a computer terminal display.

Further in accordance with a preferred embodiment of the present invention the receiving step includes receiving the request from a computer terminal connected to the network at a server connected to the network, the rendering step is performed at the server, the method further includes sending the plurality of sub-images to the computer terminal via the network, and the displaying step includes displaying the plurality of sub-images via a computer terminal display.

There is also provided in accordance with a preferred embodiment of the present invention a method for limiting the operational life of software in a network environment, the method including providing a software application with an associated password to a client via a network, receiving a request for information from the software application via the network, the request including the associated password, authenticating the password, providing the information to the software application via the network while the associated password is valid, and invalidating the password coincident with an invalidation event.

Further in accordance with a preferred embodiment of the present invention the invalidating step includes invalidating the password at a predetermined time.

Still further in accordance with a preferred embodiment of the present invention the invalidating step includes invalidating the password after a predetermined elapsed time from when the request was received.

Additionally in accordance with a preferred embodiment of the present invention the invalidating step includes invalidating the password upon the detection of a loss of communication with the client.

Moreover in accordance with a preferred embodiment of the present invention the providing step includes providing the software application in the form of an applet.

Further in accordance with a preferred embodiment of the present invention the providing step includes providing the password assembled with the software application.

Still further in accordance with a preferred embodiment of the present invention the providing step includes generating the password at a server upon receiving the request at the server.

There is also provided in accordance with a preferred embodiment of the present invention a network-based textual information system including a computer terminal operative to send a request via a network for text-editable textual information, and a server operative to receive the request, convert the text-editable textual information into a non-text-editable textual format on line upon receiving the request, and send the non-text-editable textual information to the computer terminal via the network.

Further in accordance with a preferred embodiment of the present invention the non-text-editable textual format includes a non-text-editable graphical representation of the text-editable textual information.

Still further in accordance with a preferred embodiment of the present invention the non-text-editable graphical representation includes at least one hyperlink.

Additionally in accordance with a preferred embodiment of the present invention the server further includes a first storage area that is inaccessible to the computer terminal for storing the text-editable textual information and a second storage area that is accessible to the computer terminal for storing the non-text-editable textual information.

There is also provided in accordance with a preferred embodiment of the present invention a network-based graphical information system including a computer terminal operative to send a request via a network for a graphical image, and a server operative to receive the request, render the graphical image into a plurality of sub-images on line upon receiving the request, the sub-images are displayable in a manner that is visually perceived to substantially resemble the graphical image, and send the sub-images to the computer terminal via the network.

Further in accordance with a preferred embodiment of the present invention the computer terminal is operative to display the plurality of sub-images in the manner on a display via a

video buffer the video buffer includes no more than one of the sub-images in its entirety at any given time.

Still further in accordance with a preferred embodiment of the present invention the plurality of sub-images includes a plurality of color separations of the graphical image.

Additionally in accordance with a preferred embodiment of the present invention any of the plurality of sub-images includes an interference pattern.

There is also provided in accordance with a preferred embodiment of the present invention a network-based software authentication system including a server including a password generator, password validation apparatus, a restricted-access storage area, a software application, and invalidation apparatus, the server is operative to a) cause the password generator to generate a password, b) provide the software application with the password to a client via a network, c) receive a request for information from the software application via the network, the request including the associated password, d) authenticate the password using the password validation apparatus, e) provide the information to the software application via the network while the associated password is valid, and f) invalidate the password using the invalidation apparatus coincident with an invalidation event.

Further in accordance with a preferred embodiment of the present invention the invalidation event includes the arrival of a predetermined time.

Still further in accordance with a preferred embodiment of the present invention the invalidation event includes the elapsing of a predetermined elapsed time from when the request was received.

Additionally in accordance with a preferred embodiment of the present invention the invalidation event includes the detection of a loss of communication with the client.

Moreover in accordance with a preferred embodiment of the present invention the software application includes an applet.

Further in accordance with a preferred embodiment of the present invention the password is assembled with the software application.

Still further in accordance with a preferred embodiment of the present invention the password is generated at the server upon receiving the request at the server.

It is noted that throughout the specification and claims the term "user" as it is used with respect to the use of a computer may refer to a human or surrogate therefor in combination with the computer terminal with which the human or surrogate interacts. Thus, unless otherwise specified, a reference to a user may connote a reference to the user's computer terminal, and a reference to a user's computer terminal may connote a reference to the user.

BRIEF DESCRIPTION OF THE DRAWINGS

The present invention will be understood and appreciated more fully from the following detailed description, taken in conjunction with the drawings in which:

Fig. 1 is a simplified pictorial illustration of a system for preventing unauthorized reuse of text, the system constructed and operative in accordance with a preferred embodiment of the present invention;

Fig. 2 is a simplified block diagram of server 14 of Fig. 1;

Fig. 3 is a simplified pictorial illustration of a system for preventing unauthorized reuse of graphical images, the system constructed and operative in accordance with a preferred embodiment of the present invention;

Fig. 4 is a simplified block diagram of server 34 of Fig. 3;

Figs. 5A and 5B, taken together, are simplified pictorial flow illustrations of a method of displaying the sub-images of Fig. 3;

Fig. 6 is a simplified pictorial illustration of a system for preventing unauthorized reuse of software applications, the system constructed and operative in accordance with a preferred embodiment of the present invention; and

Fig. 7 is a simplified block diagram of server 64 of Fig. 6.

DETAILED DESCRIPTION OF PREFERRED EMBODIMENTS

Reference is now made to Fig. 1 which is a simplified pictorial illustration of a system 10 for preventing unauthorized reuse of text, the system constructed and operative in accordance with a preferred embodiment of the present invention. System 10 preferably includes a communications network 12, such as the Internet, with a server 14 connected to communications network 12. A client 16 is also shown connected to communications network 12 and typically comprises any known computer terminal configured for communication via network 12 as is well known. Server 14 typically includes a storage area 18 that is accessible to clients and a storage area 20 that is not accessible to clients.

Typical operation of system 10 begins with client 16 sending a request for textual information, such as a document 22, to server 14 via network 12. The request may be made using known means, such as by selecting a hyperlink to a World Wide Web page using a browser. By "textual information" it is meant information that is to be presented as text, such as a news article or the results of a search. It is a particular feature of the invention that server 14 stores textual information in a text-editable format, such as in HTML or other known format, in storage area 20 that may not be directly accessed by clients. By "text-editable" it is meant that the textual information in its present form could be copied as text and reused, such as by pasting the copied text into a word processor and deleting words, etc.

Upon receiving the request from client 16, server 14 determines whether the textual information sought is in area 18 that is accessible to client 16, or in area 20 that is not accessible to client 16. If the textual information is in area 20, server 14 renders the textual information on line into a non-text-editable format, such as a document 24, using methods known in the art. By "non-text-editable" it is meant that the textual information in its present form could not be copied as text and reused, such as by pasting the copied text into a word processor and deleting words, etc.

For example, search results may be converted from a text-editable format to a non-text-editable format by rendering the text into a graphical format, such as GIF or JPEG, or by performing text-to-speech synthesis.

Upon rendering the textual information into a non-text-editable format, server 14 may then send the non-text-editable textual information over network 12 to client 16 where it may be output to a device such as a computer display or printer. Alternatively, server 14 may store the non-text-editable information in area 18 that is accessible to client 16. Server 12 may then generate an HTML document including a hyperlink to the rendered text and send it to client 16. Client 16 then selects the hyperlink and retrieves the rendered text from area 18. In this manner, text in HTML format that itself includes hyperlinks may be rendered into a graphical client map that preserves both the textual presentation as well as the hyperlinks.

Additional reference is now made to Fig. 2 in which server 14 is shown as typically including a filter 26 which determines whether or not requests are for textual information and whether the textual information requested is stored in area 18 or area 20. Server 14 also includes a rendering engine 28 capable of rendering HTML or other text elements to graphical format as is well known in the art. One such rendering engine is NGLAYOUT, commercially available from Netscape Communications Corporation.

Reference is now made to Fig. 3 which is a simplified pictorial illustration of a system 30 for preventing unauthorized reuse of graphical images, the system constructed and operative in accordance with a preferred embodiment of the present invention. System 30 preferably includes a communications network 32, a server 34 connected to communications network 32, and client 36, similar respectively to network 12, server 14, and client 16 as described with reference to Fig. 1 except as otherwise described herein. Server 34 typically includes a storage area 38 that is accessible to clients and a storage area 40 that is not accessible to clients.

Typical operation of system 30 begins with client 36 sending a request for a graphical image, such as an image 42, to server 34 via network 32. The request may be made using known

means, such as by selecting a hyperlink to a World Wide Web page using a browser. It is a particular feature of the invention that information that server 34 store graphical images in storage area 40 that may not be directly accessed by clients.

Upon receiving the request from client 36, server 34 determines whether the graphical image sought is in area 38 that is accessible to client 36, or in area 40 that is not accessible to client 36. If the graphical image is in area 40, server 34 decomposes the graphical image on line into a number of sub-images using methods known in the art. For example, a color image of a horse may be decomposed into a number of color-separated sub-images, such as sub-images 42A – 42C being separated into red, green, and blue components respectively, using known color separation techniques. Alternatively or additionally, interference patterns may be randomly introduced into multiple copies of an image. Any known image decomposition method may be used provided that no sub-image, when viewed independently, may be visually perceived to substantially resemble the graphical image from which it was derived.

Upon decomposing the graphical image into sub-images, server 34 may then send the sub-images 42A – 42C over network 32 to client 36 where it may be output such as via a computer display in a manner that is visually perceived to substantially resemble the original graphical image 42, such as is known in the art using techniques such as animated GIF. Alternatively, server 34 may store the sub-images in area 38 that is accessible to client 36. Server 32 may then generate an HTML document including a hyperlink to the rendered sub-images and send it to client 36. Client 36 then selects the hyperlink and retrieves the sub-images from area 18. Server 34 may also provide an applet 44 to client 36 for controlling the display of the sub-images at client 36.

Additional reference is now made to Fig. 4 in which server 34 is shown as typically including a filter 46 which determines whether or not requests are for graphical images and whether the graphical image requested is stored in area 38 or area 40. Server 34 also includes a decomposition engine 48 capable of performing color separations or introducing interference patterns into multiple copies of an image as is known in the art.

Additional reference is now made to Figs. 5A and 5B which, taken together, are simplified pictorial flow illustrations of sub-images 42A – 42C being displayed on client 36. Sub-images 42A, 42B, and 42C are shown being displayed on a computer display 52 of client 36 in succession over a time period t starting at time index t_0 and concluding at a time index t_1 of a time line 50. A video buffer 54 associated with display 52 contains the sub-image being currently displayed. It is a particular feature of the invention that at no time does video buffer 54 contain more than one entire sub-image. Fig. 5B shows the result of displaying sub-images 42A – 42C in succession over time period t, with the sub-images being visually perceived as a composite image 42' which substantially resembles graphical image 42, as is well known in the art of visual perception.

Fig. 5C is functionally equivalent to Fig. 5A with the exception that sub-images 42A – 42C of Fig. 5A are replaced with sub-images 42D, 42E, and 42F representing multiple copies of image 42 (Fig. 3) into which interference patterns 56 have been introduced. When displayed in the manner described in Fig. 5B it is believed that composite image 42' may be visually perceived to substantially resemble graphical image 42 where the interference patterns 56 are visually discounted.

Reference is now made to Fig. 6 which is a simplified pictorial illustration of a system 60 for preventing unauthorized reuse of software, the system constructed and operative in accordance with a preferred embodiment of the present invention. System 60 preferably includes a communications network 62, a server 64 connected to communications network 62, and client 66, similar respectively to network 12, server 14, and client 16 as described with reference to Fig. 1 except as otherwise described herein. Server 64 typically includes a restricted-access storage area 68, a software application such as an applet 70, and apparatus for validating passwords, such as a table 72 of valid passwords.

Typical operation of system 60 begins with client 66 sending a request for applet 70 to server 64 via network 62. The request may be made using known means, such as by selecting a hyperlink to a World Wide Web page using a browser. Upon receiving the request from client 66, server 64 preferably generates a unique password which it stores in table 72. Server 64 then sends

the applet along with the password to client 66. The password may be embedded into the applet, such as in a predetermined location within the applet code.

Client 66 may use the applet to send requests to server 64 for information stored in restricted access storage 68. The requests are preferably accompanied by the password. Upon receiving the request, server 64 authenticates the password by looking it up in table 72. If the password is valid, server 64 provides the information requested from restricted access storage 68 to client 66.

It is a particular feature of the present invention for server 64 to invalidate a password in table 72, such as by removing it from table 72, upon the occurrence of an invalidation event. Such an invalidation event may include the arrival of a predetermined time, the passage of a predetermined amount of time from when a request was last received, and the detection of a loss of communication with the client.

Additional reference is now made to Fig. 7 in which server 64 is shown as typically including a password generator 74 for generating passwords and, optionally, inserting a password, such as a password 76, into the code of applet 70. Server 64 also preferably comprises invalidation apparatus 78 for invalidating passwords as described above.

It is appreciated that components of the present invention may be implemented in computer hardware, software, or any suitable combination thereof using conventional techniques.

It is appreciated that various features of the invention which are, for clarity, described in the context of separate embodiments may also be provided in combination in a single embodiment. Conversely, various features of the invention which are, for brevity, described in the context of a single embodiment may also be provided separately or in any suitable combination.

It will be appreciated by persons skilled in the art that the present invention is not limited by what has been particularly shown and described hereinabove. Rather the scope of the present invention is defined only by the claims that follow:

CLAIMS

What is claimed is:

1. A method for providing textual information in a network environment, the method comprising:

receiving a request via a network for text-editable textual information;

converting said text-editable textual information into a non-text-editable textual format on line upon receiving said request; and

sending said non-text-editable textual information via said network.

2. A method according to claim 1 wherein said converting step comprises converting said text-editable textual information into a non-text-editable graphical representation of said text-editable textual information.

3. A method according to claim 2 wherein said converting step comprises converting said text-editable textual information into said non-text-editable graphical representation wherein said graphical representation comprises at least one hyperlink.

4. A method according to claim 1 and further comprising displaying said non-text-editable textual information via a computer terminal display.

5. A method according to claim 1 wherein said receiving step comprises receiving said request from a computer terminal connected to said network at a server connected to said network, wherein said converting step is performed at said server, and wherein said sending step comprises said server sending said non-text-editable textual information to said computer terminal via said network.

6. A method for providing graphical information in a network environment, the method comprising:

receiving a request via a network for a graphical image;

rendering said graphical image into a plurality of sub-images on line upon receiving said request, wherein said sub-images are displayable in a manner that is visually perceived to substantially resemble said graphical image; and

displaying said plurality of sub-images in said manner on a display via a video buffer wherein said video buffer comprises no more than one of said sub-images in its entirety at any given time.

7. A method according to claim 6 wherein said rendering step comprises rendering said graphical image into a plurality of color separations of said graphical image.

8. A method according to claim 6 wherein said rendering step comprises rendering said graphical image into a plurality of sub-images wherein any of said plurality of sub-images comprises an interference pattern.

9. A method according to claim 6 and further comprising sending said plurality of sub-images via said network.

10. A method according to claim 6 wherein said displaying step comprises displaying said plurality of sub-images via a computer terminal display.

11. A method according to claim 6 wherein said receiving step comprises receiving said request from a computer terminal connected to said network at a server connected to said network,

wherein said rendering step is performed at said server, wherein said method further comprises sending said plurality of sub-images to said computer terminal via said network, and wherein said displaying step comprises displaying said plurality of sub-images via a computer terminal display.

12. A method for limiting the operational life of software in a network environment, the method comprising:

providing a software application with an associated password to a client via a network;

receiving a request for information from said software application via said network, said request comprising said associated password;

authenticating said password;

providing said information to said software application via said network while said associated password is valid; and

invalidating said password coincident with an invalidation event.

13. A method according to claim 12 wherein said invalidating step comprises invalidating said password at a predetermined time.

14. A method according to claim 12 wherein said invalidating step comprises invalidating said password after a predetermined elapsed time from when said request was received.

15. A method according to claim 12 wherein said invalidating step comprises invalidating said password upon the detection of a loss of communication with said client.

16. A method according to claim 12 wherein said providing step comprises providing said software application in the form of an applet.

17. A method according to claim 12 wherein said providing step comprises providing said password assembled with said software application.

18. A method according to claim 12 wherein said providing step comprises generating said password at a server upon receiving said request at said server.

19. A network-based textual information system comprising:

a computer terminal operative to send a request via a network for text-editable textual information; and

a server operative to receive said request, convert said text-editable textual information into a non-text-editable textual format on line upon receiving said request, and send said non-text-editable textual information to said computer terminal via said network.

20. A system according to claim 19 wherein said non-text-editable textual format comprises a non-text-editable graphical representation of said text-editable textual information.

21. A system according to claim 20 wherein said non-text-editable graphical representation comprises at least one hyperlink.

22. A system according to claim 19 wherein said server further comprises a first storage area that is inaccessible to said computer terminal for storing said text-editable textual information and a second storage area that is accessible to said computer terminal for storing said non-text-editable textual information.

23. A network-based graphical information system comprising:

a computer terminal operative to send a request via a network for a graphical image; and

a server operative to receive said request, render said graphical image into a plurality of sub-images on line upon receiving said request, wherein said sub-images are displayable in a manner that is visually perceived to substantially resemble said graphical image, and send said sub-images to said computer terminal via said network.

24. A system according to claim 23 wherein said computer terminal is operative to display said plurality of sub-images in said manner on a display via a video buffer wherein said video buffer comprises no more than one of said sub-images in its entirety at any given time.

25. A system according to claim 23 wherein said plurality of sub-images comprises a plurality of color separations of said graphical image.

26. A system according to claim 23 wherein said any of said plurality of sub-images comprises an interference pattern.

27. A network-based software authentication system comprising:

a server comprising:

a password generator;

password validation apparatus;

a restricted-access storage area;

a software application; and

invalidation apparatus;

wherein said server is operative to:

a) cause said password generator to generate a password;

b) provide said software application with said password to a client via a network;

c) receive a request for information from said software application via said network, said request comprising said associated password;

d) authenticate said password using said password validation apparatus;

e) provide said information to said software application via said network while said associated password is valid; and

f) invalidate said password using said invalidation apparatus coincident with an invalidation event.

28. A system according to claim 27 wherein said invalidation event comprises the arrival of a predetermined time.

29. A system according to claim 27 wherein said invalidation event comprises the elapsing of a predetermined elapsed time from when said request was received.

30. A system according to claim 27 wherein said invalidation event comprises the detection of a loss of communication with said client.

31. A system according to claim 31 wherein said software application comprises an applet.

32. A system according to claim 27 wherein said password is assembled with said software application.

33. A system according to claim 27 wherein said password is generated at said server upon receiving said request at said server.

ABSTRACT

A method for providing textual information in a network environment, the method comprising: receiving a request via a network for text-editable textual information; converting the text-editable textual information into a non-text-editable textual format on line upon receiving the request; and sending the non-text-editable textual information via the network. Network-based systems are also disclosed.

FIG. 1

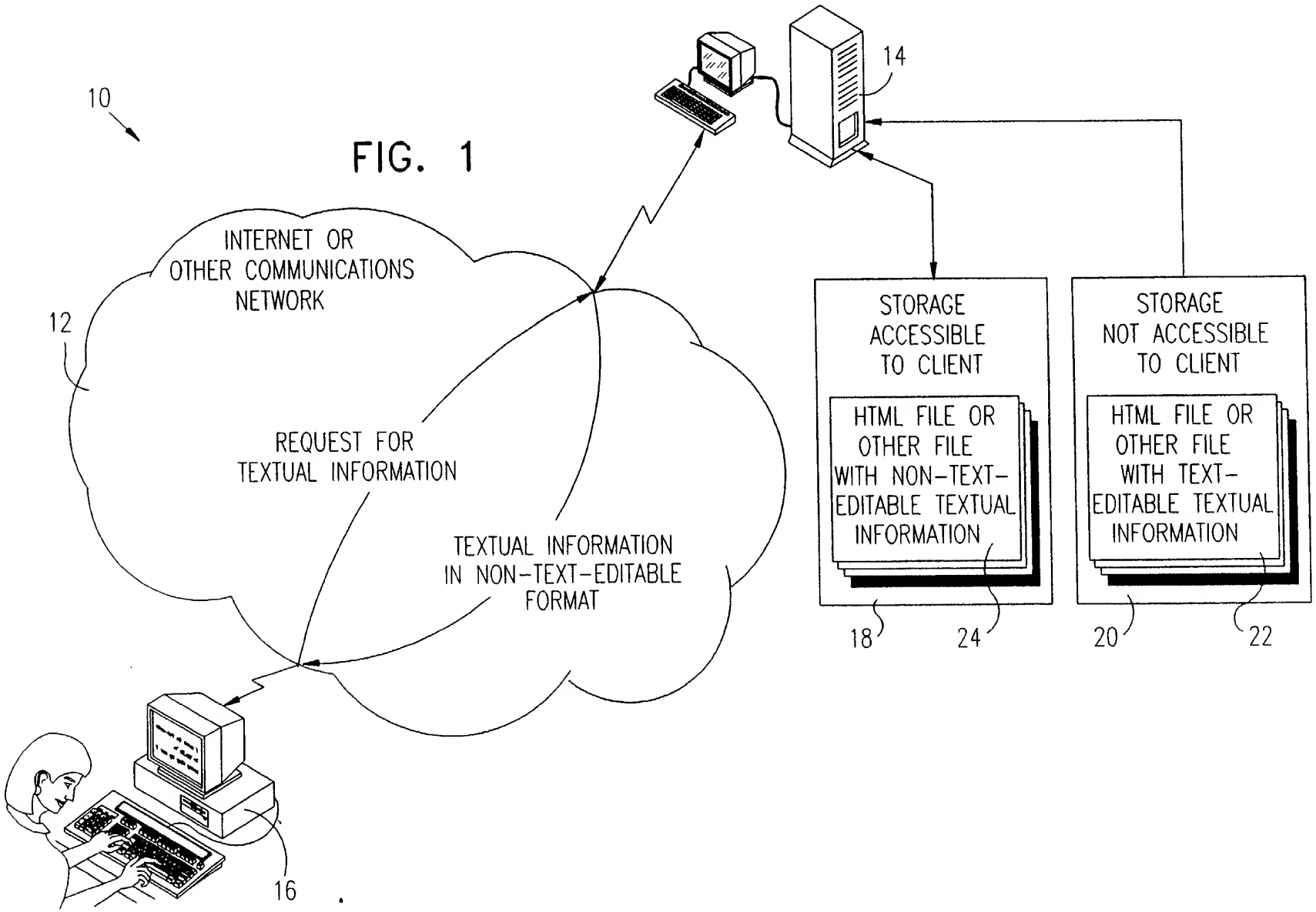

10
14
INTERNET OR
OTHER COMMUNICATIONS
NETWORK
12
REQUEST FOR
TEXTUAL INFORMATION
TEXTUAL INFORMATION
IN NON-TEXT-EDITABLE
FORMAT
STORAGE
ACCESSIBLE
TO CLIENT
HTML FILE OR
OTHER FILE
WITH NON-TEXT-
EDITABLE TEXTUAL
INFORMATION
STORAGE
NOT ACCESSIBLE
TO CLIENT
HTML FILE OR
OTHER FILE
WITH TEXT-
EDITABLE TEXTUAL
INFORMATION
18
24
20
22
16

FIG. 2

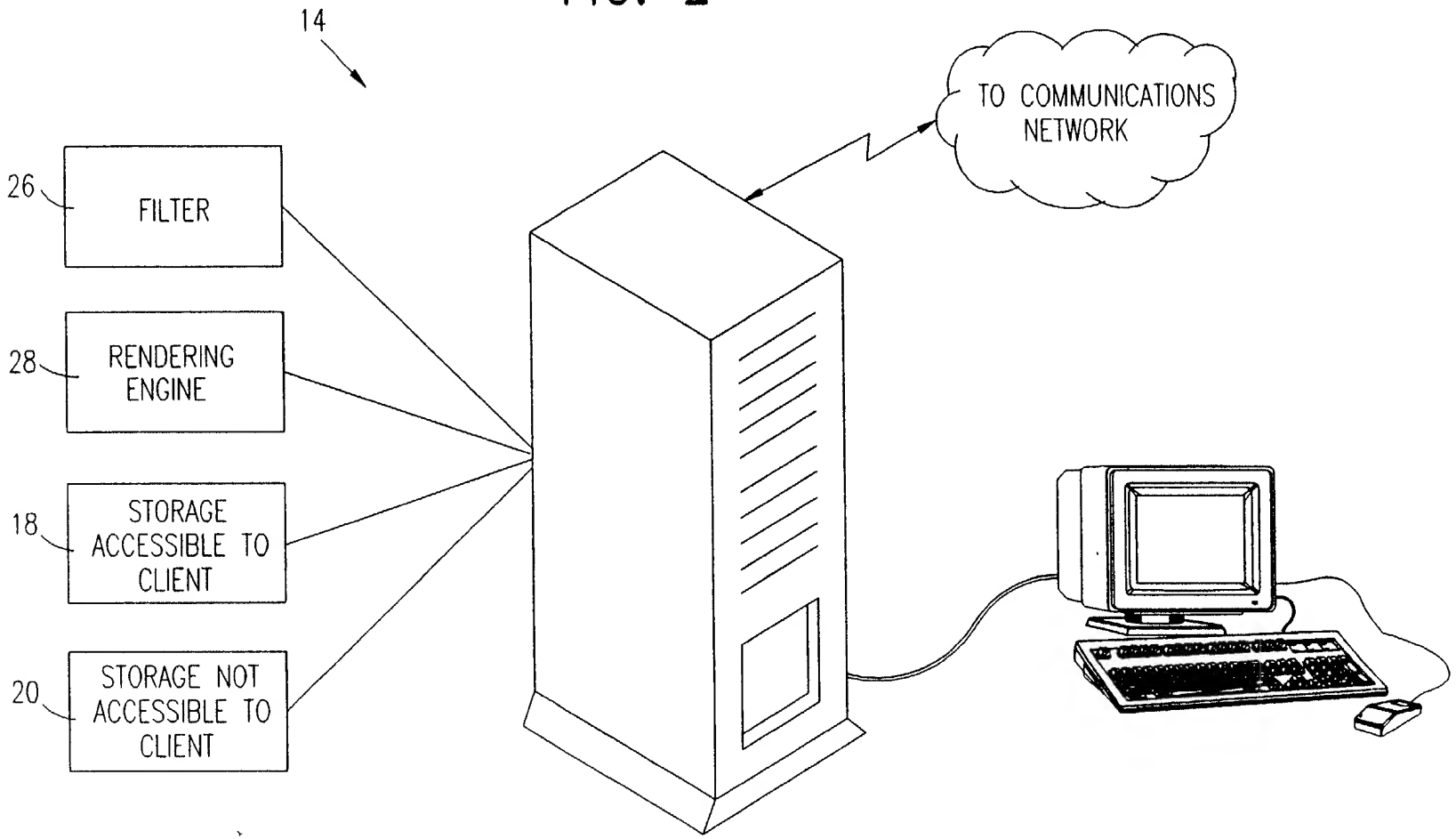

14
TO COMMUNICATIONS NETWORK
26
FILTER
28
RENDERING ENGINE
18
STORAGE ACCESSIBLE TO CLIENT
20
STORAGE NOT ACCESSIBLE TO CLIENT

FIG. 3

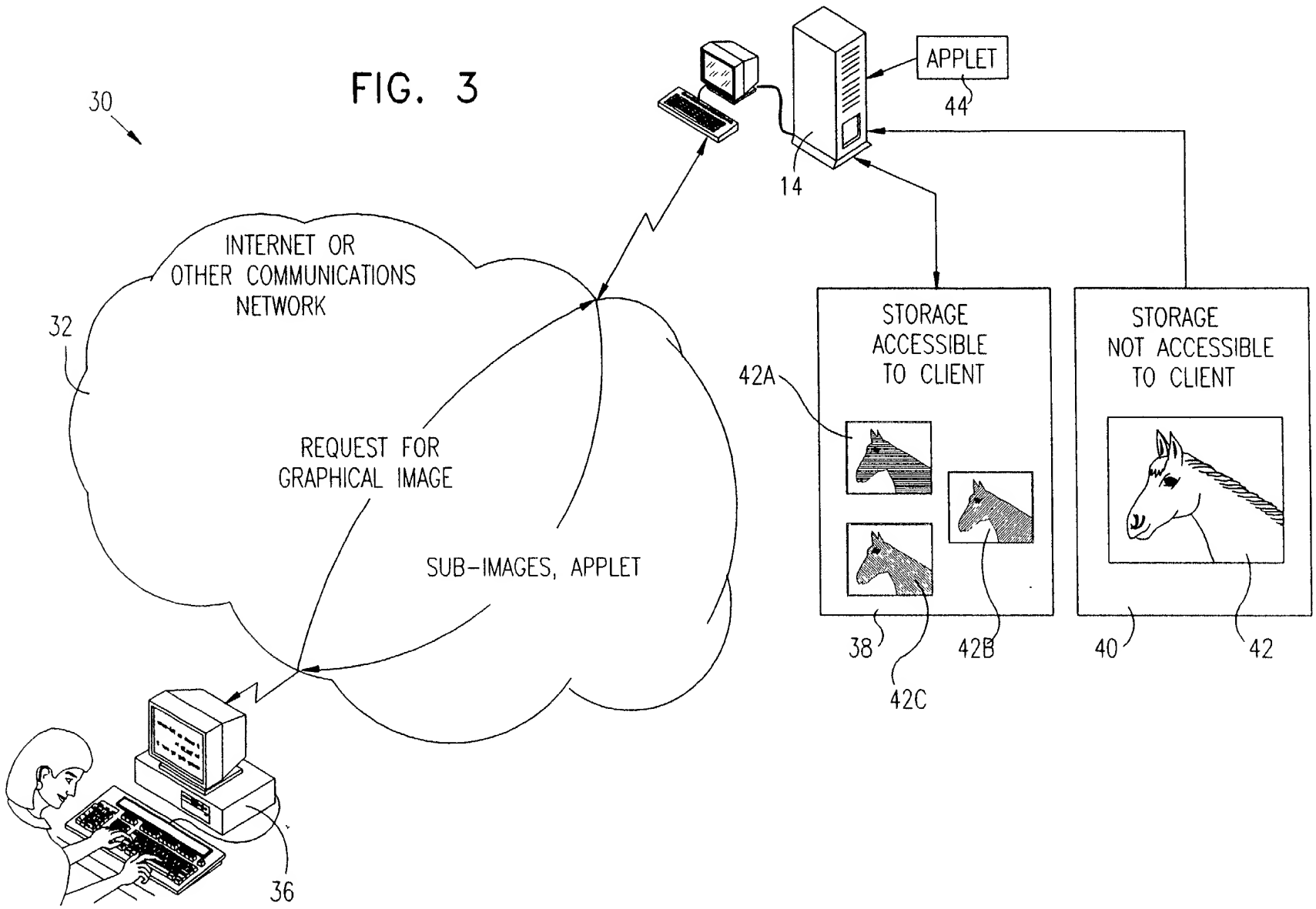
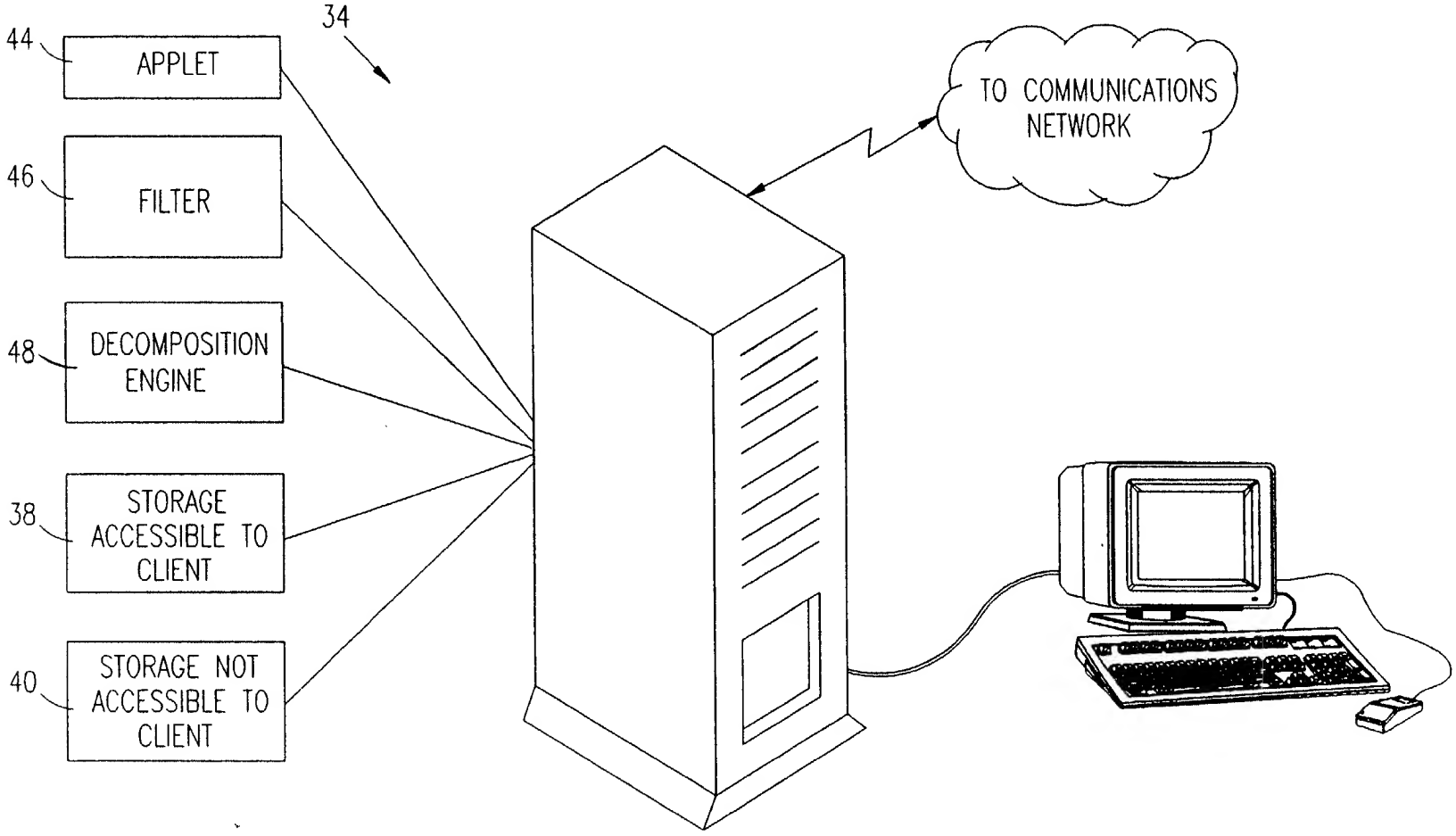

30
APPLET
44
14
INTERNET OR
OTHER COMMUNICATIONS
NETWORK
32
REQUEST FOR
GRAPHICAL IMAGE
SUB-IMAGES, APPLET
STORAGE
ACCESSIBLE
TO CLIENT
42A
STORAGE
NOT ACCESSIBLE
TO CLIENT
38
42C
42B
40
42
36

FIG. 4


34
44
APPLET
46
FILTER
48
DECOMPOSITION ENGINE
38
STORAGE ACCESSIBLE TO CLIENT
40
STORAGE NOT ACCESSIBLE TO CLIENT
TO COMMUNICATIONS NETWORK

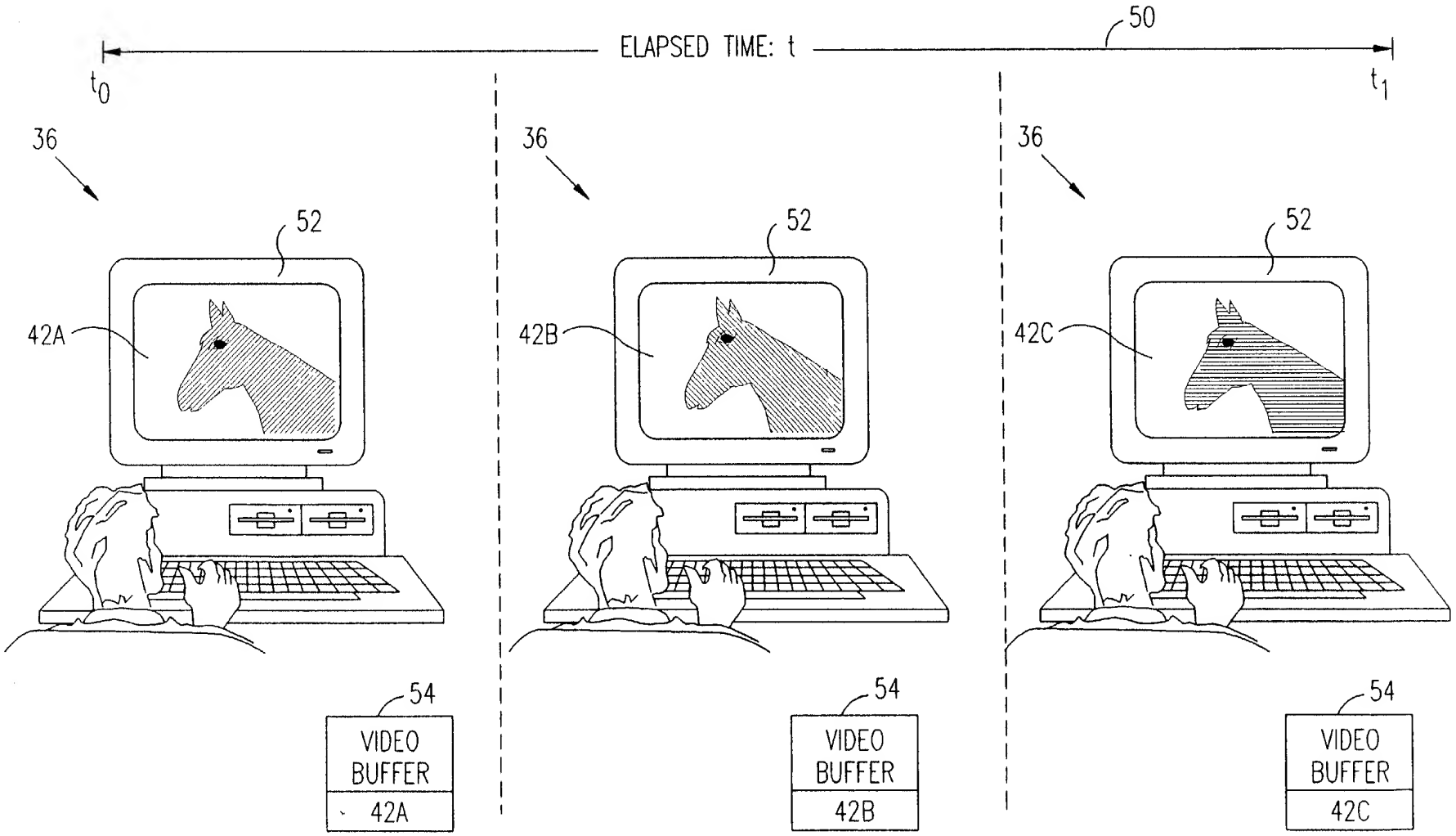
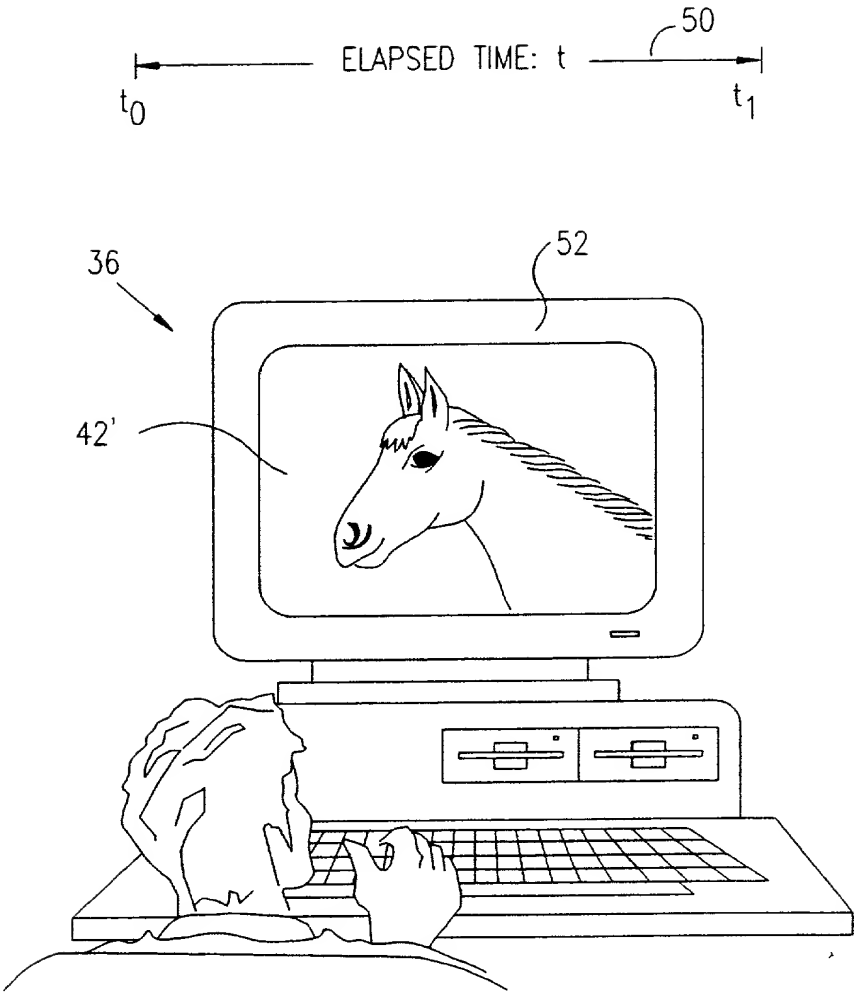

ELAPSED TIME: t
50
t_0
t_1
36
36
36
52
52
52
42A
42B
42C
54
54
54
VIDEO BUFFER
42A
VIDEO BUFFER
42B
VIDEO BUFFER
42C

FIG. 5A

FIG. 5B



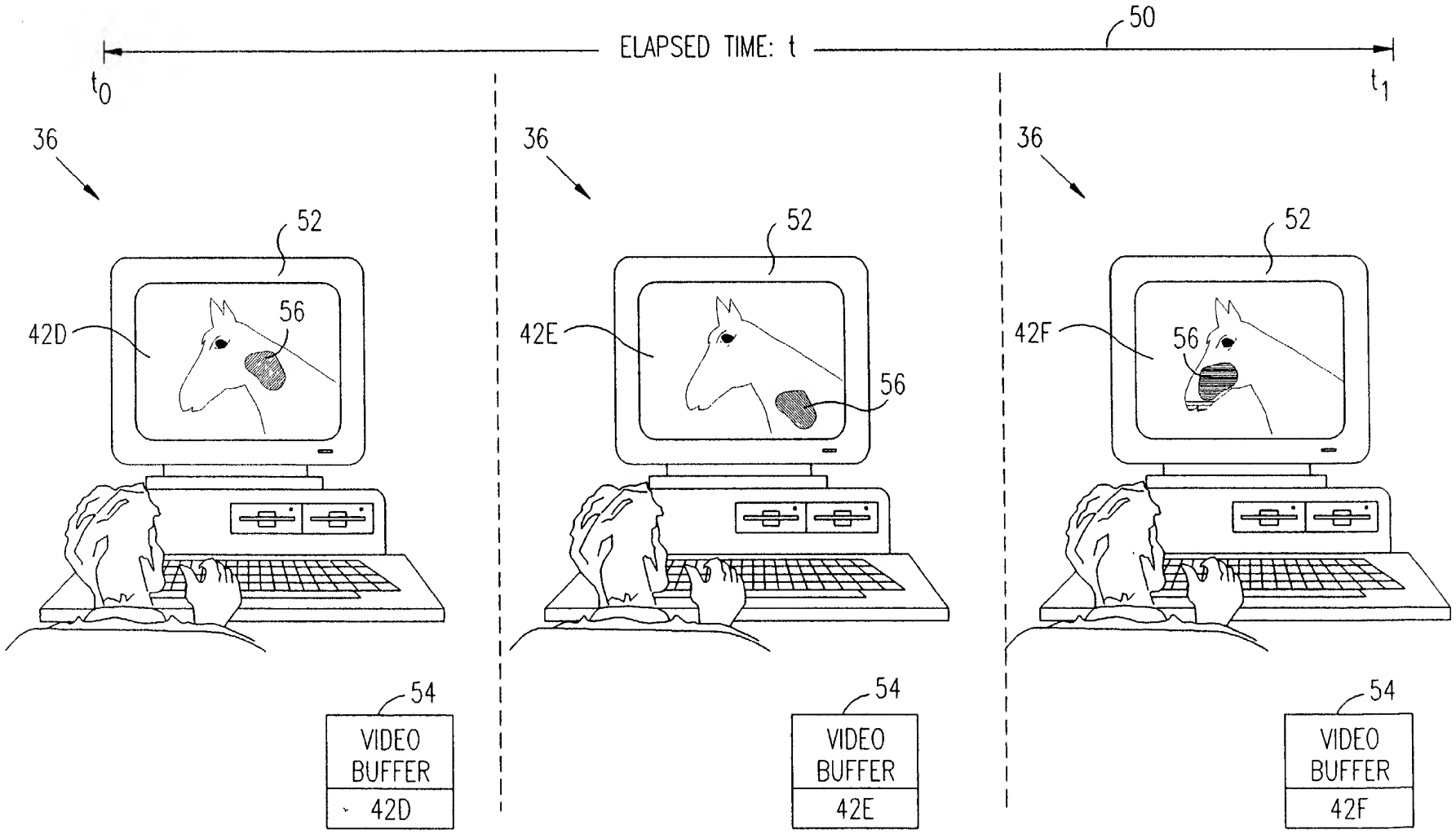

ELAPSED TIME: t
50
t_0
t_1
36
36
36
52
52
52
42D
42E
42F
56
56
56
54
54
54
VIDEO BUFFER
42D
VIDEO BUFFER
42E
VIDEO BUFFER
42F

FIG. 5C

FIG. 6

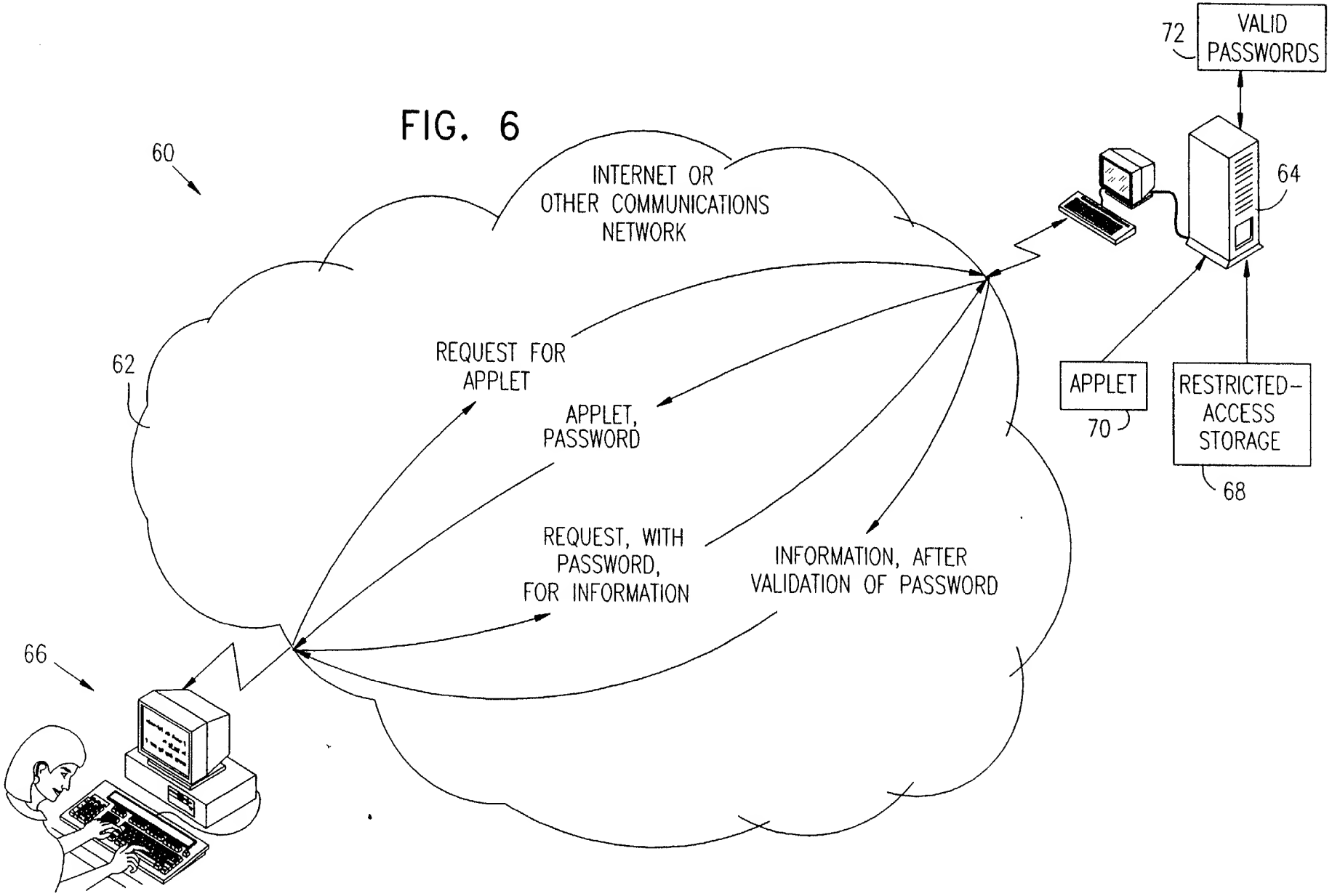
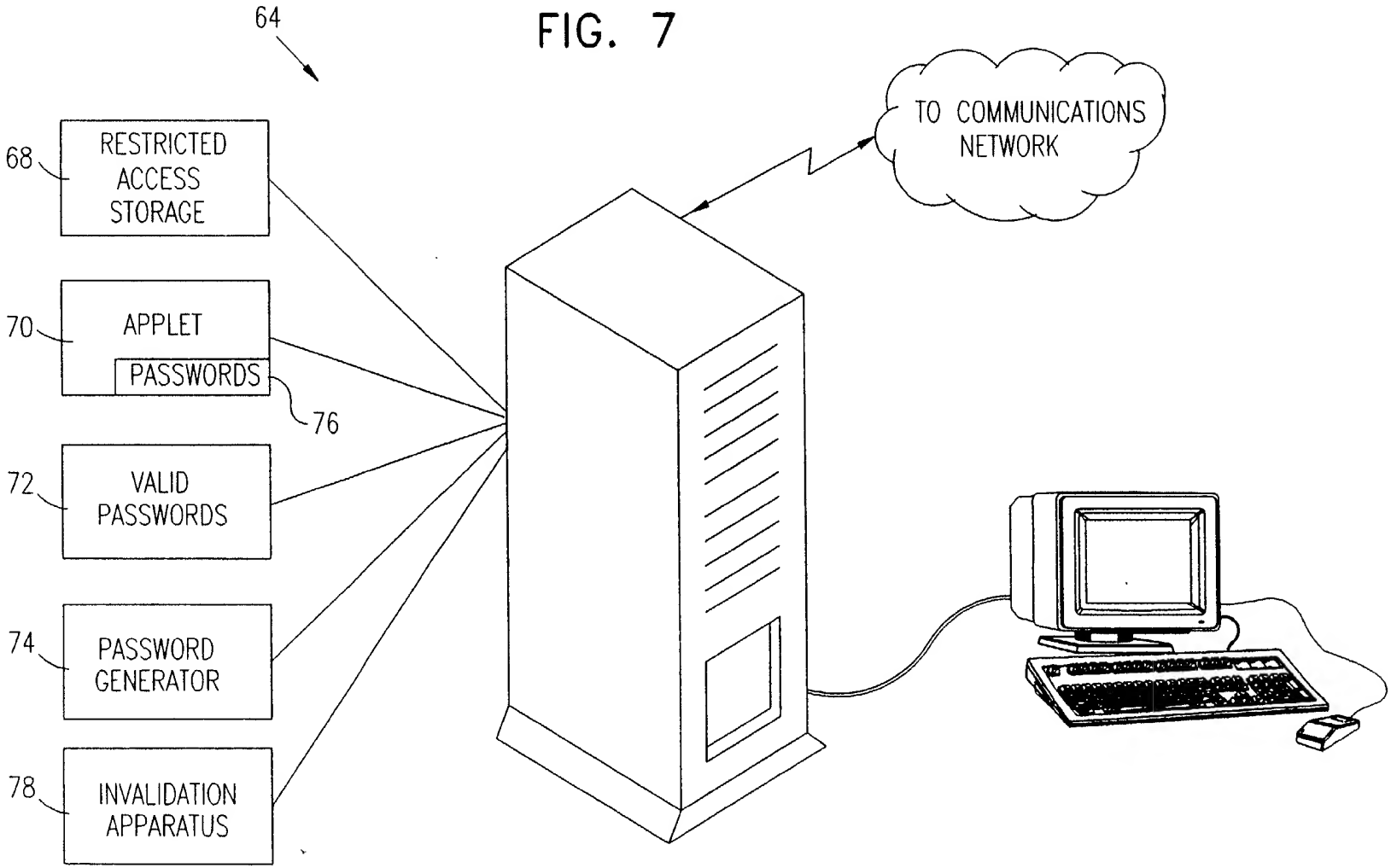

60
62
INTERNET OR
OTHER COMMUNICATIONS
NETWORK
REQUEST FOR
APPLET
APPLET,
PASSWORD
REQUEST, WITH
PASSWORD,
FOR INFORMATION
INFORMATION, AFTER
VALIDATION OF PASSWORD
66
72
VALID
PASSWORDS
64
APPLET
70
RESTRICTED-
ACCESS
STORAGE
68

FIG. 7


64
68
RESTRICTED ACCESS STORAGE
70
APPLET
PASSWORDS
76
72
VALID PASSWORDS
74
PASSWORD GENERATOR
78
INVALIDATION APPARATUS
TO COMMUNICATIONS NETWORK

DECLARATION, POWER OF ATTORNEY AND PETITION

Attorney Docket No. 6866-101XX

As a below named inventor, I hereby declare that:

My residence, post office and citizenship are as stated below next to my name.

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled: METHODS AND APPARATUS FOR PREVENTING REUSE OF TEXT, IMAGES AND SOFTWARE TRANSMITTED VIA NETWORKS

the specification of which X is attached hereto / _____ was filed on _____

as Application Serial No. _____ and was amended on _____ (if applicable).

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claims, as amended by any amendment referred to above.

I acknowledge the duty to disclose information which is material to the examination of this application in accordance with Title 37, Code of Federal Regulations, § 1.56(a).

I hereby claim foreign priority benefits under Title 35, United States Code § 119 of any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application for patent or inventor's certificate having a filing date before that of the application on which priority is claimed:

PRIOR FOREIGN APPLICATION(S)

Number	Country	Date Filed	Priority claimed Yes	Priority claimed No
124895	Israel	14 June 1998	X	

I hereby claim the benefit under Title 35, United States Code, § 120 of any United States application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35, United States Code, § 112, I acknowledge the duty to disclose material information as defined in Title 37, Code of Federal Regulations, § 1.56(a) which occurred between the filing date of the prior application and the national or PCT international filing date of this application:

Application Serial No.	Filing Date	Status (patented, pending, abandoned)

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

And I hereby appoint Billy A. Robbins, Reg. No. 18,313; Lewis M. Dalgarn, Reg. No. 20,415; Robert Berliner, Reg. No. 20,121; M. John Carson, Reg. No. 25,090; Michael S. Elkind, Reg. No. 28,710; John P. Spitals, Reg. No. 29,215; and Ying-Kit Lau, Reg. No. P35,760; all partners and associates of ROBBINS, DALGARN, BERLINER & CARSON, associate attorneys in said application, to prosecute this application and transact business in the United States Patent and Trademark Office connected with this application and I hereby give Thomas J. Lannon, Reg. No. 18,417, the power to inspect the application papers, to prosecute this application and to transact business in the United States Patent and Trademark Office connected with this application.

Please direct all correspondence and telephone calls to ROBBINS, DALGARN, BERLINER & CARSON, 201 N. Figueroa St., 5th Floor, Los Angeles, California 90012-2628; (213) 977-1001.

Wherefore I pray that Letters Patent be granted to me for the invention or discovery described and claimed in the foregoing specification and claims, and I hereby subscribe my name to the foregoing specification and claims, declaration and petition.

Full name of sole inventor: Daniel Schreiber
Inventor's signature: _____
Date: 4/5/99
Residence: Beit Shemesh, Israel
Citizenship: Israel
Post Office Address: 71 Shimon Street, Beit Shemesh 99543, Israel

Full name of second joint inventor, if any: David Guedaliah
Inventor's signature: _____
Date: 4/5/99
Residence: Beit Shemesh, Israel
Citizenship: Israel
Post Office Address: 80 Shimon Street, Beit Shemesh 99543, Israel

(Supply similar information and signature for third and subsequent joint inventors on separate page.)